Raphael Janove, Utah Bar No. 19283
Janove PLLC
500 7th Avenue, 8th Floor
New York, New York 10018
(646) 347-3940
raphael@janove.law

Liason Counsel for Plaintiff

Additional Counsel listed on Signature Block

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

DAVID ANECKSTEIN, individually and on behalf of those similarly situated, Plaintiff, v. HEALTHEQUITY, INC., Defendant.	**CLASS ACTION** **PROPOSED CLASS ACTION** **JURY TRIAL DEMANDED** Case No.

Plaintiff David Aneckstein brings this Consolidated Class Action Complaint, individually and on behalf of all others similarly situated (collectively, "Class Members"), against Defendant HealthEquity, Inc. ("HealthEquity" or "Defendant"), and alleges as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data security incident ("Data Breach") resulting from Defendant's failure to implement reasonable and industry standard data security practices.

2. Defendant manages millions of health care savings accounts and third-party health care plans for individuals across the United States, and, in so doing, maintains access to the sensitive personal information of these individuals.[1]

3. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. In providing services, Defendant collected and maintained certain personally identifiable information and/or protected health information of Plaintiff and the putative Class Members (defined below).

5. The Private Information compromised in the Data Breach included Plaintiff's and Class Members' personally identifiable information ("PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). On information and belief, the Private Information included first and last names, addresses, telephone numbers, employee IDs, name of employers, Social Security numbers, dependent information, and payment card information,[2] all of which was generated by or sent to Defendant as part of Plaintiff's and Class Member's receipt of medical services.

[1] https://www.healthequity.com/about (last visited July 31, 2024).
[2] *See* Exhibit 1, Sample Notice of Data Breach ("Notice"), found at https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773 (last visited July 31, 2024).

6. Defendant itself recognizes the importance of data security, pronouncing that "we are committed to protecting the privacy of your personal information[,]" and "[w]e use up to date administrative, physical, and technical safeguards to protect personal information."[3]

7. Despite this professed recognition, Defendant failed to take appropriate measures to safeguard the sensitive data entrusted to it from the foreseeable event of a data breach.

8. According to Defendant, "on March 25, 2024, HealthEquity [first] became aware of a systems anomaly requiring extensive technical investigation"[4] (referred to herein as the "Data Breach").

9. But it was not until June 10, 2024 that Defendant claims that it completed its investigation.[5]

10. And after determining that the Private Information of Plaintiff and Class Members was involved on June 26, 2024, Defendant failed to make this information public until it posted a notice of the Data Breach on July 29, 2024, and this notice is not even set to be sent to the 4.3 million persons affected until on or around August 9, 2024.[6]

11. Upon information and belief, Defendant's form letters to be sent Plaintiff and Class Members does not identify who the "unauthorized actor" was, address whether a ransomware demand was made and/or paid, or indicate if any of the compromised Private Information had been placed on the dark web (the illicit marketplace where thieves and criminals trade stolen PII and PHI in bulk).

---

[3] https://www.healthequity.com/privacy (last visited July 31, 2024).
[4] *See* Notice.
[5] *See* Notice.
[6] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2ec3e314-5731-49d0-a937-6dc22c6b24f3.html (last visited July 31, 2024).

12. Defendant acknowledges that its investigation discovered that it permitted the unauthorized access to and potential disclosure of "protected health information and/or personally identifiable information" of Plaintiff and Class Members which had been "stored in an unstructured data repository outside of [its] core systems."[7]

13. Upon information and belief, the Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

14. As a result of the Data Breach, Plaintiff and approximately 4.3 million Class Members,[8] suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Entities that are entrusted with healthcare patients' sensitive personally identifying information or protected health information owe a duty of care to those individuals to protect that Private Information. This duty arises because it is foreseeable that the exposure of PII and PHI to

[7] *See* Notice.
[8] *See* Notice.

unauthorized persons – especially hackers and other cybercriminals with nefarious intentions – will result in harm to the affected individuals.

16. Because of the highly sensitive nature of the data collected and maintained during the course of providing healthcare to patients, entities that maintain patients' healthcare information are leading targets for cyber-attacks. The rapid growth of electronic medical recordkeeping, online medical services, and mobile medical apps has created new pressure points for criminals to exploit.

17. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack, and Defendant itself acknowledges that this Private Information was stored in an unstructured data repository outside of its core systems.[9] The Private Information was thus maintained on in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

18. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available

[9] *See* Notice.

steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

19. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

20. Armed with the Private Information accessed in the Data Breach, data thieves immediately work to engage in identity theft and fraud and can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

21. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

22. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

23. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an

unknown third party and precisely what specific type of information was accessed.

24. Plaintiff's claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and all other similarly situated persons. Plaintiff seeks relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, breach of express contract, violation of the Utah Consumer Sales Practices Act, and unjust enrichment. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

25. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

26. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

27. Plaintiff David Aneckstein is a natural person and citizen of Pennsylvania, where he intends to remain.

28. Defendant HeathEquity, Inc. is a corporation organized under the state laws of Utah, and is in the business of providing services to individuals as part of their healthcare experience. Defendant's principal place of business is in Draper, Utah.

29. Defendant, in providing its services to Plaintiff and Class Members, is a HIPAA-covered entity ("when we are administering a health benefit plan provided by your employer, the information we collect about you is subject to the requirements of [HIPAA]").[10]

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

31. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly conducts business in Utah, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

32. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

33. Defendant HealthEquity, Inc. administers healthcare savings accounts, flexible spending accounts, health reimbursement arrangements, COBRA, in addition to other benefits, serving more than 14 million members across more than 120,000 organizations.[11]

34. Members of the proposed class here, which includes Plaintiff, provide their PII and/or PHI as part of administration of their healthcare services, and their Private Information was

[10] https://www.healthequity.com/privacy/general (General Privacy Notice) (last viewed July 31, 2024).
[11] https://www.healthequity.com/about (last visited July 31, 2024).

compromised as a result of the Data Breach ("Class Members").

35. Defendant collects and receives treatment records, lab testing data, demographic information, and payment information from Class Members and other affiliated persons. Healthcare patients entrusted Defendant with this information, either directly or indirectly through their employers, which, by its nature, is confidential and highly sensitive and may include their medical histories, current conditions, medications, Social Security numbers, account information, banking and credit card information, and other sensitive PII and PHI.

36. Because of the highly sensitive nature of the information it collects, Defendant makes many promises regarding the protection of the Private Information entrusted to it.

37. Recognizing the importance of data security, Defendant promises that "we are committed to protecting the privacy of your personal information[,]" and "[w]e use up to date administrative, physical, and technical safeguards to protect personal information."[12]

38. Plaintiff and Class Members relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. In connection with the receipt of healthcare services, individuals demand security to safeguard their Private Information, especially when PHI and other sensitive PII is involved.

39. Defendant did not keep its pledge to maintain patient privacy. Based on the nature of the Data Breach, as acknowledged by Defendant, it is apparent that Defendant's system failed to employ reasonable and appropriate security measures with regard to any or all of the following: storing data in secure, offline locations; encrypting private records and data; using up-to-date

[12] https://www.healthequity.com/privacy (last visited July 31, 2024).

software equipped with standard security patches; using anti-virus applications that block malicious code from external sources; and implementing policies requiring all workers with system access to use https protocols when using online tools.

40. Defendant's failure to adequately employ these and other industry-standard security measures needlessly exposes healthcare patients and other affiliated persons whose data was stored with Defendant to the risk of data theft.

The Data Breach

41. On March 25, 2024, Defendant first became aware of the Data Breach, which Defendant describes as "a systems anomaly requiring extensive technical investigation[.]"[13]

42. Defendant claims that it continued its investigation through June 10, 2024.[14]

43. By June 26, 2024, Defendant had determined that the Data Breach Private Information of Plaintiff and Class Members was involved.[15]

44. Defendant failed to make this information public until it posted a notice of the Data Breach incident on July 29, 2024.

45. Defendant's post notes that the Notice is set to be sent to the 4.3 million persons affected on or around August 9, 2024.[16]

46. The Private Information involved in the Data Breach includes first and last names, addresses, telephone numbers, employee IDs, name of employers, Social Security numbers,

[13] Notice.
[14] *See* Notice.
[15] *See* Notice.
[16] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2ec3e314-5731-49d0-a937-6dc22c6b24f3.html (last visited July 31, 2024).

dependent information, and payment card information.[17]

47. Upon information and belief, the cyberattack here was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

48. Plaintiff's and Class Members' Private Information was compromised and acquired in the Data Breach.

49. The files containing Plaintiff's and Class Members' Private Information that were targeted and stolen from Defendant included Plaintiff's and Class Members' PII and/or PHI.

50. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class Members.

51. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

52. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

53. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

[17] *See* Notice.

54. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

55. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/ LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

56. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[18] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ ransomware-faqs (last accessed July 31, 2024).

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

57. Given that Defendant was storing the Private Information of individuals receiving medical services, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

58. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, over 4.3 million patients, including that of Plaintiff and Class Members.[20]

Defendant Acquires, Collects, and Stores Healthcare Patients' Private Information

59. Defendant acquires, collects, and stores a massive amount of healthcare patients' Private Information provided through their receipt of healthcare services.

60. As a condition of obtaining the administration of certain healthcare services and benefits, Defendant requires that healthcare patients entrust it with highly sensitive Private Information.

61. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

---

[19] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed July 31, 2024).

[20] https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212 (last accessed July 31, 2024).

62. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

63. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and make only authorized disclosures of this information.

Defendant Knew That Cybercriminals Target Private Information

64. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information related to healthcare services, like Defendant, preceding the date of the Data Breach. Defendant knew that the sensitive personal data with which it was entrusted would be a lucrative target for hackers.

65. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyber-attacks that Defendant should have anticipated and guarded against.

66. Data breaches, including those perpetrated against entities that store Private Information related to healthcare in their systems, have become widespread.

67. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[21]

[21] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed July 31, 2024).

68. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), and Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

69. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found there were 956 medical data breaches in 2022 with over 59 million patient records exposed. This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.

70. Defendant knew and understood that unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

72. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so

notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[22]

73. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

75. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

76. As an entity in custody of current and former healthcare patients' and other affiliated persons' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however,

[22] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed July 31, 2024).

to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

77. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[24]

78. PII and PHI are valuable property rights. Their value as a commodity is measurable. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[25] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018. It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the cyber black market or the dark web, for many years.

79. The PHI/PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen

[23] 17 C.F.R. § 248.201 (2013).
[24] *Id.*
[25] *Exploring the Economics of Personal Data*, available at: https://www.oecd-ilibrary.org/exploring-the-economics-of-personal-data_5k486qtxldmq.pdf (last accessed July 31, 2024).

identity credentials.[26]

80. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, becoming more valuable to thieves and more damaging to victims.

81. For example, PII can be sold at a price ranging from $40 to $200.[27] Bad actors can purchase access to entire company data breaches from $900 to $4,500.[28]

82. PII can sell for as much as $363 per record according to the Infosec Institute.[29] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

83. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

84. PHI is particularly valuable and has been referred to as a "treasure trove for criminals" – a cybercriminal who steals a person's PHI can end up with as many as "seven to ten

---

[26] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 31, 2024).
[27] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last accessed July 31, 2024).
[28] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 31, 2024).
[29] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed July 31, 2024).

personal identifying characteristics of an individual."[30]

85. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[31]

86. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[32]

87. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

88. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[33]

89. Among other forms of fraud, identity thieves may obtain driver's licenses,

---

[30] *What Happens to Stolen Healthcare Data?*, available at: https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed July 31, 2024).

[31] *See* https://efraudprevention.net/home/education/?a=187 (last accessed July 31, 2024).

[32] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/ 03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 31, 2024).

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 31, 2024).

government benefits, medical services, and housing or even give false information to police.

90. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

Defendant Fails to Comply With FTC Guidelines

91. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

92. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[35]

---

[34] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 31, 2024).

[35] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 31, 2024).

93. The guidelines also recommend that healthcare-related businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[36]

94. The FTC further recommends that healthcare-related companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

95. The FTC has brought enforcement actions against healthcare-realted entities for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

96. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g.*, *In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (McLaren) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

[36] *Id.*

97. Defendant failed to properly implement basic data security practices.

98. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

99. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of the healthcare patients it serviced, and it was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply With HIPAA Guidelines

100. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

101. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[37] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

102. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

103. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health

[37] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

information that is kept or transferred electronically.

104. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

105. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

106. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

107. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Defendant is also required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

108. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

109. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[38]

110. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

111. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

112. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost

[38] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last accessed July 31, 2024).

effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[39] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[40]

Defendant Fails to Comply With Industry Standards

113. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which healthcare-related entities collect and maintain.

114. Several best practices have been identified that, at a minimum, should be implemented by healthcare-related entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

115. Other best cybersecurity practices that are standard in the healthcare industry

[39] US Department of Health & Human Services, Security Rule Guidance Material, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed July 31, 2024).
[40] US Department of Health & Human Services, Guidance on Risk Analysis, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed July 31, 2024).

include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

116. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

117. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one – or all – of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages

118. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.

119. As a result of Defendant's ineffective and inadequate data security practices and the resulting Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has

materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

120. Plaintiff and Class Members are at a heightened risk of identity theft for years to come. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Experian, one of the largest credit reporting companies in the world, warns consumers that identity thieves can profit off your personal information by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.

121. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

122. Because a person's identity is akin to a puzzle with multiple data points, the more

accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other crimes against the individual to obtain more data to perfect a crime.

123. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. A data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

124. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[41]

125. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an

[41] "Fullz" describes data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), available at https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last accessed July 31, 2024).

astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

126. The development of "Fullz" packages means that the stolen Private Information from the Data Breach here can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

127. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and Class Members.

128. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

129. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other Private Information (e.g., names, addresses, and dates of birth) is akin to having a master key to the gates of fraudulent activity. Data security researcher Tom Stickley, hired by companies to find flaws in their computer systems, has stated, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy

pickings."[42] Then, this comprehensive dossier can be sold—and then resold in perpetuity—to bad actors (i.e., scam telemarketers).

130. Theft of Private Information is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[43] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[44] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[45] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[46]

131. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These

[42] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say,* TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security (last accessed July 31, 2024).
[43] *Medical Identity Theft*, available at: https://www.worldprivacyforum.org/ category/med-id-theft (last accessed July 31, 2024).
[44] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, available at: https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last accessed July 31, 2024).
[45] *What To Know About Medical Identity Theft*, available at: https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed July 31, 2024).
[46] *Id.*

changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime. For example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed due to medical activities of the imposter; and victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[47]

132. There may also be a time lag between when sensitive personal information is stolen, when it is illicitly used, and when a person discovers the illicit usage. For example, it takes approximately three months on average for consumers to discover that their identity has been

[47] *The Geography of Medical Identity Theft*, available at: ttps://www.worldprivacy forum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_ Theft_fs.pdf (last accessed July 31, 2024).

stolen and used, but it takes some individuals up to three years to learn that information.

133. It is within this context that Plaintiff and Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

134. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified that their Private Information has been compromised, as in this Data Breach, a reasonable person is expected to take steps and time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose an individual to greater financial harm – ultimately, the resource and asset of time has been lost.

135. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

136. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their accounts for fraudulent activity and checking their credit reports for unusual activity.

137. Plaintiff and Class Members' mitigation efforts, including those who experience actual identity theft and fraud, are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches, the GAO Report, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit

record."[48]

138. Plaintiff's mitigation efforts are also consistent with the steps that the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (if someone steals their identity, an extended fraud alert that lasts for seven years is suggested), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[49]

Diminution of Value of Private Information

139. PII and PHI are valuable property rights.[50] Their value is axiomatic, considering the value of an individual's data in today's economy and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

140. A robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[51]

141. In fact, the data marketplace is so sophisticated that consumers can actually sell their

---

[48] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), available at: https://www.gao.gov/new.items/d07737.pdf (last accessed Apr. 30, 2024).

[49] *See* Federal Trade Commission, *Identity Theft.gov*, available at: https://www.identitytheft.gov/Steps (last accessed July 31, 2024).

[50] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[51] *See* https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed July 31, 2024).

non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[52,53]

142. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[54]

143. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

144. Thus, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

145. Among other forms of fraud, identity thieves may obtain driver's licenses, which can then lead to improper procurement of government benefits, medical services, and housing, and even giving false information to police.

146. The fraudulent activity resulting from the Data Breach may not come to light for

[52] https://datacoup.com/ (last accessed July 31, 2024).
[53] https://digi.me/what-is-digime/ (last accessed July 31, 2024).
[54] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed July 31, 2024).

years.

147. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

148. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to the detailed Private Information of, upon information and belief, 4.3 million individuals, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

149. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

150. Given the type of targeted attack in this case and related sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes (e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims).

151. Such fraud may go undetected until debt collection calls commence months, or even

years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

152. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

153. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of the Benefit of the Bargain

154. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of healthcare-related services, directly or indirectly, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF'S EXPERIENCES

155. Plaintiff David Aneckstein receives healthcare-related services from Defendant.

156. Plaintiff has held a Health Savings Account ("HSA") with HealthEquity for over ten years for himself and his children.

157. In order to obtain these healthcare-related services from Defendant, Plaintiff was

required to provide Defendant with Plaintiff's PII and PHI.

158. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

159. Plaintiff is very careful about sharing Plaintiff's sensitive Private Information. Plaintiff stores any documents containing Plaintiff's Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted Plaintiff's Private Information to Defendant had Plaintiff known of Defendant's inadequate data security policies.

160. Upon information and belief, Plaintiff's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach.

161. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including monitoring Plaintiff's accounts for fraudulent activity and checking credit reports for unusual activity. Plaintiff has also changed his passwords for his online HSA account. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

162. Plaintiff suffered actual injury from having Plaintiff's Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly

increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

163. The Data Breach has caused Plaintiff to suffer fear, substantial anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed Plaintiff of key details about the Data Breach's occurrence.

164. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

165. As a result of the Data Breach, Plaintiff is at a present and continued increased risk of identity theft and fraud for years to come.

166. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

167. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

168. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

> All persons in the United States whose PII and/or PHI was compromised as a result of the Data Breach.

169. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

170. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

171. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

172. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is currently unknown to Plaintiff and exclusively in the possession of Defendant, according to Defendant, approximately 4.3 million persons were impacted in the Data Breach.[55] Thus, the Class is sufficiently numerous to warrant certification.

173. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA and/or HIPAA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

[55] *See* Notice.

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

174. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

175. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

176. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common

issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

177. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find the cost of litigating their individual claims to be prohibitively high and would thus have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

178. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to Class Members such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

179. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence

180. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

181. Defendant requires healthcare patients, including Plaintiff and Class Members, to submit non-public PII and PHI in the ordinary course of providing its healthcare-related services.

182. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of servicing healthcare patients, which services affect commerce.

183. Plaintiff and Class Members entrusted Defendant with their Private Information and understood that Defendant would safeguard their information.

184. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

185. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a reasonable duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

186. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

187. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

188. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

189. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the healthcare patients it services. That special relationship arose because Plaintiff and Class Members entrusted Defendant with their confidential Private Information, a necessary part of receiving services related to healthcare from Defendant. Moreover, Defendant was in an exclusive position to know the extent of its data security capabilities and to detect and prevent the Data Breach.

190. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

191. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

192. Defendant also had a duty to exercise appropriate clearinghouse practices to remove

former healthcare patients' Private Information that it was no longer required to retain pursuant to regulations.

193. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

194. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

195. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. Defendant's specific negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
b. Failing to adequately monitor the security of their networks and systems;
c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' Private Information;
e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' Private Information that it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

196. Defendant violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

197. Plaintiff and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

198. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

199. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

200. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

201. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

202. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

203. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

204. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

205. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

206. Plaintiff and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

207. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

208. Defendant's duty extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

209. Defendant has admitted that the Private Information of Plaintiff and Class Members was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

210. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

211. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

212. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the Private Information.

213. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

214. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

215. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

216. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

217. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract

218. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

219. Plaintiff and Class Members were required to provide their Private Information to

Defendant as a condition of receiving healthcare-related services from Defendant.

220. Plaintiff and Class Members entrusted their Private Information to Defendant. Defendant accepted Plaintiff's and Class Members' personal medical information for the purpose of providing services for Plaintiff and Class Members, thereby entering an implied contract whereby Defendant became obligated to reasonably safeguard Plaintiff's and Class Members' personal medical information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

221. Implicit in the agreement between Defendant and Plaintiff and Class Members to provide Private Information, was Defendant's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

222. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

223. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

224. In accepting the Private Information of Plaintiff and Class Members, Defendant

understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

225. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

226. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

227. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

228. Plaintiff and Class Members, through their use of Defendant's services, caused money to be paid Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

229. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

230. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

231. Plaintiff and Class Members fully and adequately performed their obligations under

the implied contracts with Defendant.

232. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information, and by failing to timely delete certain Private Information, and by failing to provide accurate notice that Private Information was compromised as a result of the Data Breach.

233. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

234. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

235. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Express Contract

236. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

237. As discussed above, Defendant affirmatively agreed to protect the security of the PII and PHI provided to it by healthcare patients. These express representations appeared in Privacy policy and its General Privacy Notice.

238. Defendant's data security promises were a material term of Plaintiff's and Class Members' agreement to utilize Defendant hospital for healthcare-related services.

239. Defendant breached its express contractual obligations to reasonably protect and secure the PII and PHI of Plaintiff and Class Members.

240. Defendant's breach caused damages to Plaintiff and Class Members, including nominal damages.

COUNT IV
Violation of Utah Consumer Sales Practices Act

241. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein and brings this count on behalf of themselves and the Class.

242. Defendant's conduct alleged above constitutes deceptive acts or practices in connection with a consumer transaction under Utah Code section 13-11-1 *et seq*. Defendant's conduct was at all material times developed, orchestrated, and implemented in part out of their headquarters in Utah by their senior management in conjunction with those under their direct control.

243. The Utah Consumer Sales Practice Act is intended to protect consumers and, as much as possible, conform Utah state law to policies of the Federal Trade Commission Act.

244. The purchase of Defendant's services satisfies the definition of a consumer transaction in that it required Plaintiffs and Class Members to expend money, directly or indirectly, on the provision of Defendant's services.

245. Defendant violated Utah Code section 13-11-1(a)'s proscription against indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not. Defendant indicated that it would protect Plaintiff and Class Members Private Information, but it has not.

246. Defendant made affirmative representations to protect the security of Plaintiff's and Class Members' Private Information, but Defendant failed to implement measures to protect their Private Information, failed to identify foreseeable security risks and vulnerabilities in its network, failed to take reasonable steps to mitigate and defend against the threat posed by the threat actor, and failed to notify Plaintiff and Class Members of the Data Breach in a timely manner.

247. Defendant omitted and actively concealed material facts regarding its inadequate security policies and practices from Plaintiff and Class Members and withheld and continues to withhold information regarding the nature and extent of the Data Breach. Had Defendant disclosed that its data systems lacked the almost universal safeguards described above, Plaintiff and Class Members would not have allowed Defendant to collect and maintain their Private Information.

248. Defendant's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate

causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and Class Members that their Private Information was accessed by unauthorized persons in the Data Breach.

249. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class Members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiff's and Class Members' Private Information and other Defendant data was vulnerable.

250. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

251. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

252. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices, and regarding the security of the sensitive PII and PHI. Defendant also did not disclose information regarding the length of time that it maintains persons' Private Information and other records. Likewise, during the days, weeks, and months following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

253. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiff's and Class Members' PII and PHI.

254. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former patients' and other affiliated persons' Private Information.

255. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety

and confidentiality of their Private Information.

256. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

257. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

258. Defendant generated revenue by way of Plaintiff and Class Members paying or generating healthcare-related payments where Defendant was the direct beneficiary of these payments. Defendant's services were of lesser quality and value than Defendant represented in that Defendant did not take reasonable measures to safeguard customers' personal medical information. In reliance on Defendant's misrepresentations about its products and services, Plaintiff and Class Members entered transactions that they would not have, or for which Plaintiff and Class Members would have paid less, or nothing at all, but for Defendant's representations.

259. The injuries suffered by Plaintiff and Class Members greatly outweigh any potential countervailing benefit to patients/consumers or to competition and are not injuries that Plaintiff and Class Members should have reasonably avoided.

260. If not for Defendant's deceptive acts or practices or unconscionable acts or practices in violation of the Act, Plaintiffs and Class Members would not have paid for Defendant's services.

261. Plaintiff and Class Members are entitled to recover $2,000 in statutory fines or their damages caused by Defendant's violation of Utah Code § 13-11-1 *et seq*. pursuant to Utah Code section 13-11-19 (2) and (4). They are further entitled to a declaratory judgment that Defendant's

acts and practices described herein violate Utah Code section 13-11-1 *et seq*. pursuant to Utah Code section 13-11-19 (1) (a) and (3). Defendant's acts and practices described herein violate Utah Code section 13-11-1 *et seq*. Finally, Plaintiff and Class Members are entitled to an award of attorneys' fees under Utah Code section 13-11-19 (5).

262. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class Members as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

263. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT V
Unjust Enrichment

264. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

265. This count is pleaded in the alternative to Plaintiff's breach of implied and express contract claims above (Count II and Count III).

266. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they, directly or indirectly, paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

267. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form of their Private Information as well as payments made by them or on their behalf as a necessary part of their receiving healthcare-related services. Defendant accepted and realized that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

268. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

269. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

270. Defendant, however, diverted funds intended to be applied towards data security to its own profit and failed to adequately fund its data security program sufficient to secure Plaintiff's and Class Members' Private Information from unauthorized access and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

271. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

272. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

273. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

274. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

275. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

276. Plaintiff and Class Members have no adequate remedy at law.

277. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

278. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

279. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that Defendant unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. Prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as

well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. Appointing a qualified and independent third party assessor, for a period of ten years, to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: July 31, 2024

Respectfully submitted,

/s/ Raphael Janove

Raphael Janove, Utah Bar No. 19283
Janove PLLC
500 7th Avenue, 8th Floor

New York, New York 10018
(646) 347-3940
raphael@janove.law

Liason Counsel for Plaintiff

Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM
950 W. University Drive, Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Counsel for Plaintiff and the Putative Class